The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)

February 11, 2009

Timothy A. Hall

Sharon S. Keller

National Institute of Standards and Technology

Information Technology Laboratory

Computer Security Division

TABLE OF CONTENTS

1 Introduction

This document, *The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)*, specifies the procedures for validating implementations of the Galois/Counter Mode (GCM), an algorithm for authenticated encryption with associated data, and its specialization, GMAC, for generating a message authentication code (MAC) on data that is not encrypted, as specified in SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC* [1]. The GCMVS is designed to perform automated testing on Implementations Under Test (IUTs).

This document defines the purpose, the design philosophy, and the high-level description of the validation process for GCM and GMAC. The requirements and administrative procedures to be followed by those seeking formal validation of an implementation of SP800-38D are presented. The requirements described include a specification of the data communicated between the IUT and the GCMVS, the details of the tests that the IUT must pass for formal validation, and general instruction for interfacing with the GCMVS.

A set of GCM test vectors is available at http://csrc.nist.gov/groups/STM/cavp/documents/mac/gcmtestvectors.zip.

2 Scope

This document specifies the tests required to validate IUTs for conformance to the Galois/Counter Mode (GCM) and GMAC, as specified in [1]. When applied to an IUT, the GCMVS provides testing to determine the correctness of the implementation of the GCM/GMAC algorithm specifications. As detailed in the standard, there is both an authenticated encryption function and an authenticated decryption function. The authenticated encryption function allows for the generation of the IV to occur internally or externally. A separate test suite has been designed for each of these functions and verifies that an IUT has implemented the components of the function according to the specifications in the standard.

The GCMVS validation process requires additional prerequisite testing of the underlying approved symmetric key block cipher with a block size of 128 bits, such as the Advanced Encryption Standard (AES) algorithm that is specified in Federal Information Processing Standard (FIPS) Pub. 197 [2].

3 Conformance

The successful completion of the tests contained within the GCMVS and the AESAVS is required to be validated as conforming to the SP800-38D standard. Testing for the cryptographic module in which GCM is implemented is defined in FIPS PUB 140-2, Security Requirements for Cryptographic Modules [2].

4 Definitions and Abbreviations

4.1 Definitions

DEFINITION	**MEANING**
AAD	Additional Authenticated Data.
Additional Authenticated Data	The input data to the authenticated encryption function that is authenticated but not encrypted
Authenticated Decryption	The function of GCM in which the ciphertext is decrypted into the plaintext, and the authenticity of the ciphertext and the AAD is verified.
Authenticated Encryption	The function of GCM in which the plaintext is encrypted into the ciphertext and an authentication tag is generated on the AAD and the ciphertext.
Authentication Tag (Tag)	A cryptographic checksum on data that is designed to reveal both accidental errors and the intentional modification of the data.
CMT laboratory	Cryptographic Module Testing laboratory that operates the GCMVS
Forward Cipher Function	A permutation on blocks that is determined by the choice of a key for a given block cipher.

4.2 Abbreviations

ABBREVIATION	**MEANING**
AES	Advanced Encryption System
AESAVS	Advanced Encryption System Algorithm Validation System

FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
IUT	Implementation Under Test

5 Design Philosophy of Galois/Counter Mode Validation System

The GCMVS is designed to test conformance to GCM and GMAC specifications rather than provide a measure of a product's security. The validation tests are designed to assist in the detection of accidental implementation errors, and are not designed to detect intentional attempts to misrepresent conformance. Thus, validation should not be interpreted as an evaluation or endorsement of overall product security.

The GCMVS has the following design philosophy:

1. The GCMVS is designed to allow the testing of an IUT at locations remote to the GCMVS. The GCMVS and the IUT communicate data via *REQUEST* and *RESPONSE* files. The GCMVS also generates *SAMPLE* files to provide the IUT with a sample of what the *RESPONSE* file should look like.

2. The testing performed within the GCMVS utilizes statistical sampling (i.e., only a small number of the possible cases are tested); hence, the successful validation of a device does not imply 100% conformance with the standard.

6 Galois/Counter Mode Validation System (GCMVS) Test

The GCMVS tests the implementation of the GCM/GMAC algorithm for its conformance to the SP800-38D standard. When applied to an IUT, the GCMVS provides testing to determine the correctness of the implementation of the authenticated encryption and/or the authenticated decryption function specifications. A separate test suite has been designed for each of these functions. Within the authenticated encryption function, a separate test suite has been designed based on the IV source – internally or externally generated. The validation test suite for each function verifies that an IUT has implemented the components of the function according to the specifications in the standard.

The GCM algorithm validation process requires additional prerequisite testing of the underlying AES algorithm using any mode of operation that uses the forward cipher function.

6.1 Configuration Information

To initiate the validation process of the GCMVS, a vendor submits an application to an accredited laboratory requesting the validation of its implementation of the GCM and/or GMAC algorithm. The vendor's implementation is referred to as the Implementation Under Test (IUT). The request for validation includes background information describing the IUT along with information needed by the GCMVS to perform the specific tests. More specifically, the request for validation includes:

1. Cryptographic algorithm implementation information

    a. Vendor Name;

    b. Product Name;

    c. Product Version;

    d. Implementation in software, firmware, or hardware;

    e. Processor and Operating System with which the IUT was tested if the IUT is implemented in software, or Processor if the IUT is a firmware implementation;

    f. Brief description of the IUT or the product/product family in which the IUT is implemented by the vendor (2-3 sentences); and

2. Configuration information for the GCMVS tests.

    a. Source of IV – internal or external

    b. IV lengths supported – 96 bits, minimum and maximum bit sizes

    c. PT lengths supported – minimum and maximum bit sizes

    d. AAD lengths supported – minimum and maximum bit sizes

    e. Tag lengths supported in bits (128, 120, 112, 104, 96, 64, 32)

6.2 The Validation Test for the Authenticated Encryption Function

6.2.1 IV Generated Externally

The file generated is called gcmEncryptExtIV128(192/256).req

Within each request file, there is a section for each combination of Key length, IV length, PT length, AAD length, and Tag Length. For each of these combinations, the Authenticated Encryption with IV Test provides the lengths of each of the parameters listed above and 15 sets of data for these variables to the IUT. The IUT uses these values to

generate the ciphertext CT and Tag values.

All of the values generated by the IUT are stored in the response file in the format specified in the sample file. There shall be a response file for every sample file.

The GCMVS will verify the correctness of the IUT's values by comparing them to the known values generated by the GCMVS. If they match, the GCMVS records a value of PASS; otherwise, the GCMVS records a value of FAIL.

6.2.2 IV Generated Internally

The file generated is called gcmEncryptIntIV128(192/256).req

Within each request file, there is a section for each combination of Key length, IV length, PT length, AAD length, and Tag Length. For each of these combinations, the Authenticated Encryption without IV Test provides the lengths of each of the parameters listed above and 15 sets of data for these variables to the IUT. The IUT supplies an IV to be used with each set of values to generate the CT and Tag values.

All of the values generated by the IUT are stored in the response file in the format specified in the sample file. There shall be a response file for every sample file.

The GCMVS will verify the correctness of the IUT's values by using the IUT-supplied IV and computing the CT and Tag values. The GCMVS compares the CT and Tag values to the values generated by the IUT. If they match, the GCMVS records a value of PASS; otherwise, the GCMVS records a value of FAIL.

6.3 The Validation Test for the Authenticated Decryption Function

The file generated is called gcmDecrypt128(192/256).req

Within each request file, there is a section for each combination of Key length, IV length, PT length, AAD length, and Tag Length. For each of these combinations, the Decryption Validation Test provides the lengths of each of the parameters listed above and 15 sets of data for these variables to the IUT. Within these sets of data, the GCMVS will modify one variable value to introduce an error. Errors will be introduced in either the ciphertext (CT) or the Tag. Approximately half of the cases will be correct; the other half will have errors.

The IUT uses this information to validate the GCMVS Tag value returning a PASS or FAIL in the response file. If the IUT returns a PASS, they also shall return a PT value. All of the values generated by the IUT are stored in the response file in the format specified in the sample file. There shall be a response file for every sample file.

This validation test determines whether or not the IUT can detect errors in the decryption process.

The GCMVS verifies that the correct responses are returned by the IUT. If they match, the GCMVS records a value of PASS; otherwise, the GCMVS records a value of FAIL.

Appendix A References

[1] *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, Special Publication 800-38D, National Institute of Standards and Technology, November 2007.

[2] *Security Requirements for Cryptographic Modules*, FIPS Publication 140-2, National Institute of Standards and Technology, May 2001.